AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A message encryption system comprising:

a binding component that creates a remote service binding between a user's digital certificate and a remote service associated with a target system, the remote service binding specifying:

the remote service by specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed, and

that the user's digital certificate is to be used when a dialog is initiated between the initiator system and the remote service;

a session key generator that generates a session key for a dialog between the initiator system and the remote service at the target system, the session key employed to securely exchange a message associated with the dialog; and,

an encryption component that employs asymmetric encryption to encrypt the session key using a private key associated with the initiator system to yield a first session key encryption, encrypt the first session key encryption using the public key specified by the remote service binding to yield an encrypted session key output and securely transmit the encrypted session key output to the target system, the session key thereafter being employed to encrypt the message and securely exchange the message between the initiator system and the target system, wherein the encryption component encrypts the message using the session key to yield a first message encryption, and subsequently encrypts the first message encryption using the private key associated with the initiator system to yield an encrypted message output.

2. (Original) The system of claim 1, the session key comprising a 128-bit randomly generated symmetric key.

3. (Cancelled)

4. (Cancelled)

5. (Previously Presented) The system of claim 1, the remote service binding created at the initiator system using the following syntax:

Create Remote Service Binding <LOGICAL SERVICE NAME>
To Service '<SERVICE>'
With (User = [< USER>])

where <LOGICAL SERVICE NAME> is a logical name assigned to the service by the binding, <SERVICE> is the remote service, and <USER> is an identification of the user whose public key is to be utilized when a dialog is initiated with the remote service by the initiator system.

6. (Previously Presented) The system of claim 1, further comprising a plurality of trusted agents that act as a proxy for a publisher to respectively exchange the message with respective subscribers, the trusted agents employing the private key.

7. (Previously Presented) The system of claim 6, a trusted agent negotiates a unique session key with a subscriber.

8. (Original) The system of claim 6, the trusted agents acting in concert to dynamically load balance distribution for the publisher.

9. (Previously Presented) The system of claim 1, the public key being stored as a digital certificate.

10. (Original) The system of claim 9, the digital certificate being associated with a user *via* a login protocol.

11. (Previously Presented) The system of claim 1, the encryption component separately encrypts the session key with a public key associated with the target system, and the

separate encryption is provided as an output to the target system together with the encrypted session key output.

12-13. (Cancelled).

14. (Currently Amended) A message decryption system comprising:

a session key employed to securely exchange a message associated with a dialog between an initiator system and a remote service running on a target system, the session key twice encrypted using a private key associated with the initiator system and a public key specified according to a remote service binding that associates the public key with the remote service running on the target system, the remote service binding specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed; and,

a decryption component that receives the encrypted version of the session key from the initiator system, employs asymmetric decryption to decrypt the encrypted session key using a private key associated with the target system to yield a first session key decryption, and decrypts the first session key decryption using a public key associated with the initiator system to yield the session key, the session key thereafter being employed to decrypt a received encoded version of the message, wherein the decryption component decrypts the encoded version of the message using the session key to yield a first message decryption, and subsequently decrypts the first message decryption using the public key associated with the initiator system to yield the message.

15. (Previously Presented) The system of claim 14, the message comprising a digital certificate employed as part of a broker service security system.

16. (Previously Presented) The system of claim 14, the private key being securely associated with the target system.

17. (Cancelled)

18. (Currently Amended) A method facilitating session key encryption comprising:

employing a processor executing computer-executable instructions stored on a computer-readable storage medium to implement the following acts:

establishing a remote service binding at a first system that binds a service running on a second system with a particular user's digital certificate, the remote service binding specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed;

initiating a dialog at the first system with the service running on the second system;

identifying the digital certificate bound to the service upon initiating the dialog; firstly encrypting a symmetric session key with a private key associated with an initiator of the dialog to yield a first encryption;

secondly encrypting a result of the first encryption with a public key associated with the identified digital certificate to yield a second encryption;

transmitting a result of the first encryption from the first system to the second system; and

employing the session key to encrypt and decrypt messages between the first system and the second system that access the service running on the second system.

19. (Previously Presented) The method of claim 18, further comprising encrypting a message at the first system using the session key to yield a first message encryption, and encrypting the first message encryption at the first system using the private key associated with the identified digital certificate to yield a twice-encrypted message.

20. (Original) The method of claim 18, the public key being associated with a target of a message.

21. (Original) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 18.

22. (Currently Amended) A method facilitating session key decryption comprising:

employing a processor executing computer-executable instructions stored on a computer-readable storage medium to implement the following acts:

establishing a dialog between a dialog initiator and a service running on a target system;

receiving at the target system an encrypted session key from the dialog initiator, the encrypted session key encrypted using a private key associated with the dialog initiator and a public key specified by a remote service binding that associates the public key with the service running on the target system, the remote service binding specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed;

decrypting the encrypted session key with a private key associated with the target system to yield a first decryption;

decrypting the first decryption with a public key associated with the dialog initiator to yield the decrypted session key;

employing the decrypted session key together with the public key associated with the dialog initiator to decrypt a subsequent twice-encrypted message from the dialog initiator;

deploying multiple instances of a service broker that serve to establish dialogs between subscribers and the dialog initiator;

sharing the private key associated with the dialog initiator with the multiple instances of the service broker; and

negotiating a unique session key with each of a subscriber accessing one of the multiple instances of the service broker.

23. (Original) The method of claim 22, the private key being associated with a target of a message.

24. (Original) The method of claim 22, the public key being associated with an initiator of a message.

25. (Original) A computer readable medium having stored thereon computer executable instructions for carrying out the method of claim 22.

26. (Currently Amended) A computer-readable storage medium encoded with a data structure that facilitates secure distributed communication, the data structure comprising:

a first data field comprising a remote service binding that associates a service running on a remote system with a particular user's public key; and

a data field comprising an encrypted session key, the session key encrypted using a private key associated with an initiator of a message to the service and the public key associated with the service by the remote service binding, the remote service binding specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed;

a data field comprising an encrypted message, the encrypted message first encrypted with the session key, then encrypted with the private key associated with the initiator of the message, the message comprising a digital certificate that is employed as part of a service broker security system that facilitates location transparency of the service.

27. (Currently Amended) A message decryption system comprising:

means for creating a remote service binding that associates a service running on a first system with a particular public key, the remote service binding specifying a logical address of the remote service such that the binding is not dependent on the physical location of the service or the number of instances of the service that are deployed;

means for initiating a message exchange between the first system and a second system, the message exchange involving access to the service running on the first system;

means for receiving an encrypted session key from the second system, the encrypted session key encrypted using a private key associated with the second system and the public key associated with the service by the remote service binding;

means for decrypting the encrypted session key using a private key associated with the first system to yield a first decryption;

means for decrypting the first decryption with a public key associated with the second system to yield a second decryption;

means for securely storing a result of the second decryption as a session key; and

means for employing the session key to decrypt an encrypted message received by the second system, the encrypted message encrypted using the session key and a private key securely associated with the second system.

28. (Previously Presented) The system of claim 1, further comprising multiple instances of the broker service sharing the same private key such that an application accessing the remote service treats the multiple instances collectively as a unit.